Symantec.250-587.v2026-10-08.q44

Exam Code:	250-587
Exam Name:	Symantec Data Loss Prevention 16.x Administration Technical Specialist
Certification Provider:	Symantec
Free Question Number:	44
Version:	v2026-10-08
# of views:	107
# of Questions views:	453
https://www.freecram.net/torrent/Symantec.250-587.v2026-10-08.q44.html	

NEW QUESTION: 1
Which tool must a DLP administrator run to certify the database prior to upgrading DLP?
A. Lob_Tablespace Reclamation Tool
B. Upgrade Readiness Tool
C. SymDiag
D. EnforceMigrationUtility
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 2
Which two automated response rules will be active in policies that include Exact Data Matching (EDM) detection rule? (Choose two.)
A. Endpoint Discover: Quarantine File
B. Network Protect: Quarantine File
C. Endpoint Prevent: Block
D. All: Send Email Notification
E. Endpoint Prevent: User Cancel
Answer: (SHOW ANSWER)

NEW QUESTION: 3
A customer needs to integrate information from DLP incidents into external Governance, Risk and Compliance dashboards.
Which feature should a third party component integrate with to provide dynamic reporting, create custom incident remediation processes, or support business processes?
A. A Web incident extraction report
B. Export incidents using the CSV format
C. Incident Data Views

D. Incident Reporting and Update API
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which two Network Discover/Cloud Storage targets apply Information Centric Encryption as policy response rules?
A. SQL Databases
B. Microsoft Exchange
C. Microsoft SharePoint
D. Network File System (NFS)
E. Windows File System
Answer: (SHOW ANSWER)

NEW QUESTION: 5
How should a DLP administrator exclude a custom endpoint application named "custom_app.exe" from being monitoring by Application File Access Control?
A. Add "custom_app.exe" to the "Application Whitelist" on all Endpoint servers.
B. Add "custom_app.exe" Application Monitoring Configuration and de-select all its channel options.
C. Add "custom_app_.exe" as a filename exception to the Endpoint Prevent policy.
D. Add "custom_app.exe" to the "Program Exclusion List" in the agent configuration settings.
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 6
Which of the following actions can you implement ONLY as a Smart Response rule (and not as an automates response rule)?
A. All: Limit Incident Data Retention
B. All: Add Note
C. Network Protect: SharePoint Release From Quarantine
D. All: Set Attribute
Answer: (SHOW ANSWER)

NEW QUESTION: 7
What detection server is used for Network Discover, Network Protect, and Cloud Storage?
A. Network Protect Storage Discover
B. Network Discover/Cloud Storage Discover
C. Network Prevent/Cloud Detection Service
D. Network Protect/Cloud Detection Service
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 8

A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported.
What should the administrator do to allow incidents to be generated against this file?
A. Change the "Ignore requests Smaller Than" value to 1
B. Add the filename to the Inspect Content Type field
C. Change the "PacketCapture.DISCARD_HTTP_GET" value to "false"
D. Uncheck trial mode under the ICAP tab
Answer: A (LEAVE A REPLY)
References:

NEW QUESTION: 9
Which two actions are available for a "Network Prevent: Remove HTTP/HTTPS content" response rule when the content is unable to be removed? (Choose two.)
A. Redirect the content to an alternative destination
B. Remove the content through FlexResponse
C. Encrypt the content before posting
D. Allow the content to be posted
E. Block the content before posting
Answer: (SHOW ANSWER)

NEW QUESTION: 10
An administrator is unable to log in to the Enforce management console as "sysadmin". Symantec DLP is configured to use Active Directory authentication. The administrator is a member of two roles: "sysadmin" and "remediator." How should the administrator log in to the Enforce console with the "sysadmin" role?
Freecram.net
A. sysadmin\username@domain
B. username\sysadmin
C. sysadmin\username
D. domain\username
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which two locations can Symantec DLP scan and perform Information Centric Encryption (ICE) actions on? (Choose two.)
A. Exchange
B. Jiveon
C. File store
D. SharePoint
E. Confluence
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 12
What is the recommended ratio of Enforce servers to Oracle database servers when deploying Symantec DLP?
A. 1:1
B. 1:2
C. 2:1
D. 3:1
Answer: (SHOW ANSWER)
Symantec DLP uses a one-to-one relationship between an Enforce server and its Oracle database. The database is not intended to be shared concurrently by multiple independent Enforce servers, and a single Enforce deployment does not require multiple Oracle database servers. This 1:1 association provides a clear ownership boundary for policies, incidents, configuration information, system events, user administration, and reporting data managed by the Enforce server. Detection servers communicate with Enforce, while Enforce persists and retrieves the operational information stored in its assigned Oracle database. Consequently, each Enforce server must have its corresponding Oracle database server, establishing the recommended ratio of 1:
1. The product-name typing error in the candidate document has also been corrected from "DPL" to "DLP."

NEW QUESTION: 13
What is required on the Enforce server to communicate with the Symantec DLP database?
A. Port 8082 should be opened
B. CryptoMasterKey.properties file
C. Symbolic links to .dbf files
D. SQL*plus Client
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 14
A DLP administrator has added several approved endpoint devices as exceptions to an Endpoint Prevent policy that blocks the transfer of sensitive data. However, data transfers to these devices are still being blocked.
What is the first action an administrator should take to enable data transfers to the approved endpoint devices?
A. Double-check that the correct device ID or class has been entered for each device
B. Verify Application File Access Control (AFAC) is configured to monitor the specific application
C. Edit the exception rule to ensure that the "Match On" option is set to "Attachments"
D. Disable and re-enable the Endpoint Prevent policy to activate the changes
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which detection method depends on "training sets"?
A. Form Recognition
B. Vector Machine Learning (VML)
C. Index Document Matching (IDM)

D. Exact Data Matching (IDM)
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 16
Which detection method is best suited for identifying sensitive content within scanned images or image-based PDF files?
A. Keyword-Based Detection
B. Optical Character Recognition (OCR)
C. Regular Expression Matching
D. Exact Data Matching (EDM)
Answer: (SHOW ANSWER)
Optical Character Recognition is required when sensitive information exists as pixels rather than directly extractable text. A scanned document or image-based PDF may visibly contain names, account numbers, identification numbers, or other protected information, but normal detection rules cannot evaluate those characters until they have been converted into machine-readable text. OCR performs that conversion and passes the extracted text to the DLP detection process, where keywords, regular expressions, Data Identifiers, or other policy rules can inspect it. Keyword and regular-expression matching may operate after OCR processing, but neither technique performs the image-to-text conversion. Exact Data Matching also requires readable and normalized values before comparing content with an index. Therefore, Optical Character Recognition, option B, is the correct detection method.

Valid 250-587 Dumps shared by EduDump.com for Helping Passing 250-587 Exam! EduDump.com now offer the **newest 250-587 exam dumps**, the EduDump.com 250-587 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 250-587 dumps with Test Engine here: https://www.edudump.com/exams/Symantec/250-587/premium/ (**110** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
What is one difference between Exact Data Matching (EDM) and Exact Match Data Identifiers (EMDI)?
A. EDM rules can be evaluated by the DLP Agent and EMDI rules cannot.
B. EDM is better at detecting non-standard delimiters (in ID numbers) than EMDI.
C. EDM requires an index and EMDI does not.
D. EDM is its own detection rule type and EMDI is a Data Identifier validation check.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
A compliance officer needs to understand how the company is complying with its data security policies over time. Which report should be compliance officer generate to obtain the compliance information?
A. Policy Trend report, summarized by policy, then quarter

B. Policy report, filtered on date and summarized by policy
C. Policy Trend report, summarized by policy, then severity
D. Policy report, filtered on quarter and summarized by policy
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Why would an administrator set the Similarity Threshold to zero when testing and tuning a Vector Machine Learning (VML) profile?
A. To capture the matches to the Positive set
B. To see the false negatives only
C. To capture the matches to the Negative set
D. To see the entire range of potential matches
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which two (2) detection servers are available as virtual appliances? (Choose two.)
A. Network Monitor
B. Optical Character Recognition (OCR)
C. Network Prevent for Email
D. Network Discover
E. Network Prevent for Web
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
Under the "System Overview" in the Enforce management console, the status of a Network Monitor detection server is shown as "Running Selected." The Network Monitor server's event logs indicate that the packet capture and filereader processes are crashing.
What is a possible cause for the Network Monitor server being in this state?
A. The Network Monitor server's license file has expired.
B. There is insufficient disk space on the Network Monitor server.
C. The Enforce and Network Monitor servers are running different versions of DLP.
D. The Network Monitor server's certificate is corrupt or missing.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
What is Application Detection Configuration?
A. The Cloud Detection Service (CDS) process that tells Enforce a policy has been violated
B. The Data Loss Prevention (DLP) policy which has been pushed into Cloud Detection Service (CDC) for files in transit to or residing in Cloud apps
C. The terminology describing the Data Loss Prevention (DLP) process within the CloudSOC administration portal

D. the setting configured within the user interface (UI) that determines whether CloudSOC should send a file to Cloud Detection Service (CDS) for analysis.
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 23
A compliance officer needs to understand how the company is complying with its data security policies over time.
Which report should be compliance officer generate to obtain the compliance information?
A. Policy Trend report, summarized by policy, then quarter
B. Policy Trend report, summarized by policy, then severity
C. Policy report, filtered on quarter and summarized by policy
D. Policy report, filtered on date and summarized by policy
Answer: (SHOW ANSWER)

NEW QUESTION: 24
A software company wants to protect its source code, including new source code created between scheduled indexing runs.
Which detection method should the company use to meet this requirement?
A. Exact Data Matching (EDM)
B. Described Content Matching (DCM)
C. Vector Machine Learning (VML)
D. Indexed Document Matching (IDM)
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 25
Which two technologies should an organization utilize for integration with the Network Prevent products?
(choose two.)
A. Network Tap
B. Network Firewall
C. Proxy Server
D. Mail Transfer Agent
E. Encryption Appliance
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 26
Which type of response rule does Cloud Service for Email use to block confidential emails?
A. Cloud Applications and API Appliance: Redact Data-in-Motion
B. Network Prevent: Block SMTP Message
C. Network Prevent: Block HTTP/HTTPS

D. Cloud Applications and API Appliance: Block Data-in-Motion
Answer: (SHOW ANSWER)

NEW QUESTION: 27
A DLP administrator needs to remove an agent and its associated events from an Endpoint server.
Which Agent Task should the administrator perform to disable the agent's visibility in the Enforce management console?
A. Disable action from Symantec Management Console
B. Delete action from the Agent Health dashboard
C. Change Endpoint Server action from the Agent Overview page
D. Delete action from the Agent List page
Answer: (SHOW ANSWER)

NEW QUESTION: 28
A DLP administrator is preparing to install Symantec DLP and has been asked to use an Oracle database provided by the Database Administration team.
Which SQL *Plus command should the administrator utilize to determine if the database is using a supported version of Oracle?
A. select database version from < database name > ;
B. select * from db$version;
C. select * from v$version;
D. select db$ver from < database name > ;
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 29
A DLP administrator needs to remove an agent its associated events from an Endpoint server.
Which Agent Task should the administrator perform to disable the agent's visibility in the Enforce management console?
A. Change endpoint Server action from the Agent Overview page
B. Delete action from the Agent health dashboard
C. Delete action from the Agent List page
D. Disable action from Symantec Management Console
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Where should an administrator set the debug levels for an Endpoint Agent?
A. Setting the log level within the Agent List
B. Advanced configuration within the Agent settings
C. Setting the log level within the Agent Overview
D. Advanced server settings within the Endpoint server

Answer: (SHOW ANSWER)

References:

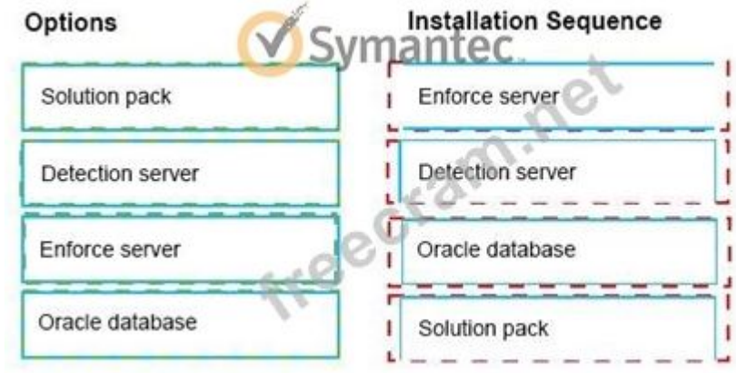
NEW QUESTION: 31

What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

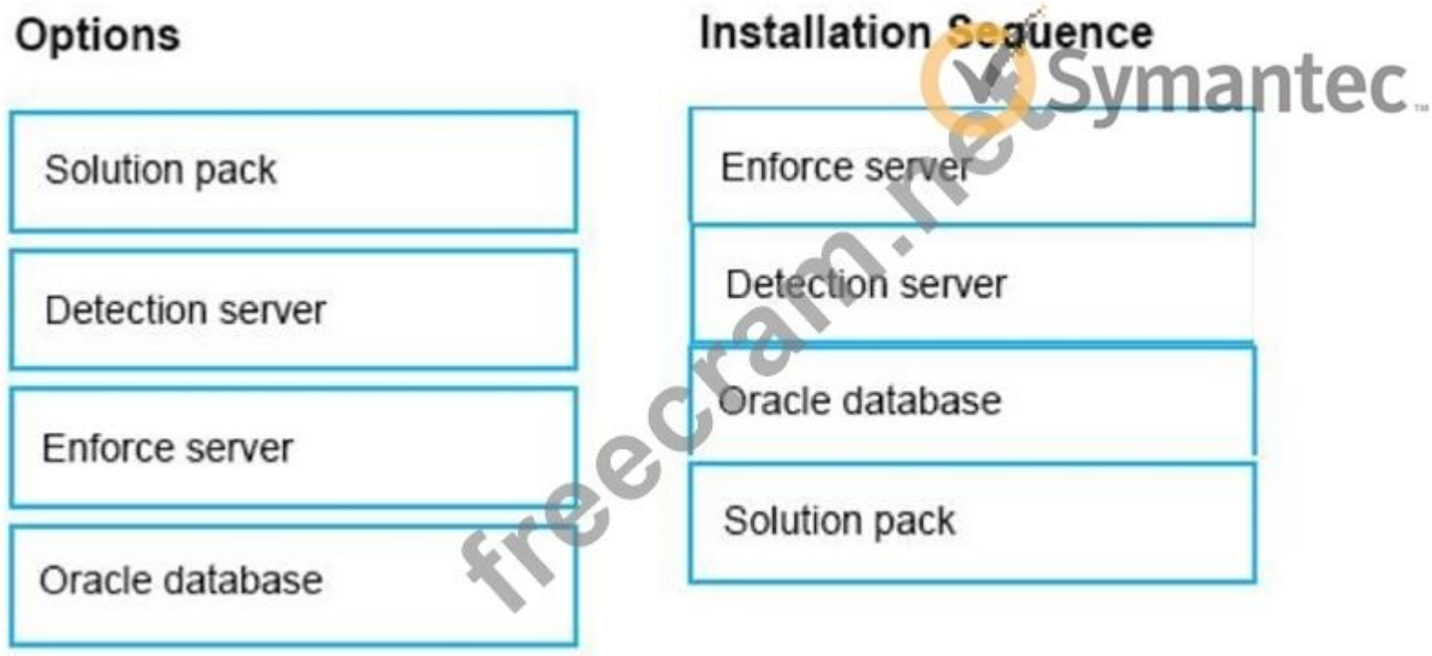
Place the options in the correct installation sequence.



Answer:



Explanation:



Valid 250-587 Dumps shared by EduDump.com for Helping Passing 250-587 Exam! EduDump.com now offer the **newest 250-587 exam dumps**, the EduDump.com 250-587 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 250-587 dumps with Test Engine here: https://www.edudump.com/exams/Symantec/250-587/premium/ (**110** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
Where do you configure the list of Endpoint Servers (or load balancers) to which a DLP Agent can report?
A. In the Agent Package
B. In the Agent Group
C. In the Agent Overview
D. In the Agent Configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 33
What is the correct order for data in motion when a customer has integrated their CloudSOC and DLP solutions?
A. User > Enforce > CloudSOC > Application
B. User > Enforce > Application
C. User > CloudSOC Gatelet > Enforce > Application
D. User > CloudSOC Gatelet > DLP Cloud Detection Service > Application
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
A DLP administrator created a new agent configuration for an Endpoint server. However, the endpoint agents fail to receive the new configuration.
What is one possible reason that the agent fails to receive the new configuration?
A. The new agent configuration was copied and modified from the default agent configuration.
B. The Endpoint server needs to be recycled so that the new agent configuration can take effect.
C. The new agent configuration was saved but not applied to any endpoint groups.
D. The default agent configuration must be disabled before the new configuration can take effect.
Answer: (SHOW ANSWER)

NEW QUESTION: 35
A company needs to implement Data Owner Exception so that incidents when employees send or receive their own personal information.
What detection method should the company use?
A. Indexed Document Matching (IDM)
B. Vector Machine Learning (VML)
C. Exact data matching (EDM)
D. Described Content matching (DCM)
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 36
A DLP administrator created a new agent configuration for an Endpoint server. However, the endpoint agents fail to receive the new configuration.
What is one possible reason that the agent fails to receive the new configuration?
A. The new agent configuration was saved but not applied to any endpoint groups.
B. The Endpoint server needs to be recycled so that the new agent configuration can take effect.
C. The default agent configuration must be disabled before the new configuration can be assigned.
D. The new agent configuration was copied and modified from the default agent configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
What detection method utilizes Data Identifiers?
A. Indexed Document matching (IDM)
B. Described Content Matching (DCM)
C. Directory Group Matching (DGM)
D. Exact Data Matching (EDM)
Answer: D (LEAVE A REPLY)
References:

NEW QUESTION: 38

Why would an administrator set the Similarity Threshold to s=zero when testing and tuning a Vector Machine Learning (VML) profile?

A. To capture the matches to the Positive set

B. To capture the matches to the negative set

C. To see the false negatives only

D. To see the entire range of potential matches

Answer: (SHOW ANSWER)

References:

NEW QUESTION: 39

Which server target uses the "Automated Incident Remediation Tracking" feature in Symantec DLP?

A. Exchange

B. File System High-Speed Discovery

C. File System (standard)

D. SharePoint

Answer: (SHOW ANSWER)

NEW QUESTION: 40

Which action should a DLP administrator take to secure communications between an on-premises Enforce server and detection servers hosted in the Cloud?

Freecram.net

A. Use the built-in Symantec DLP certificate for the Enforce Server, and use the "sslkeytool" utility to create certificates for the detection servers.

B. Use the built-in Symantec DLP certificate for both the Enforce server and the hosted detection servers.

C. Set up a Virtual Private Network (VPN) for the Enforce server and the hosted detection servers.

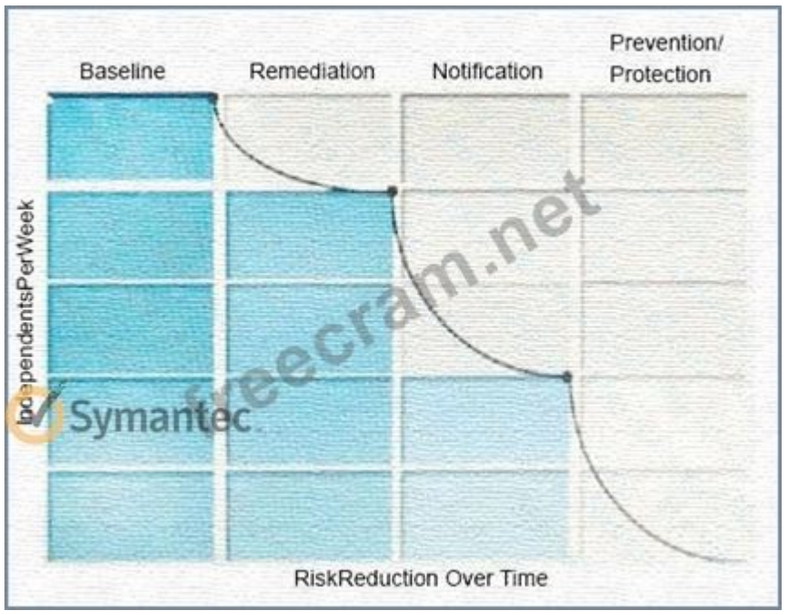
D. Use the "sslkeytool" utility to create certificates for the Enforce server and the hosted detection servers.

Answer: A (LEAVE A REPLY)

References:

NEW QUESTION: 41

Refer to the exhibit.



What activity should occur during the baseline phase, according to the risk reduction model?

A. Test policies to ensure that blocking actions minimize business process disruptions

B. Define and build the incident response team

C. Monitor incidents and tune the policy to reduce false positives

D. Establish business metrics and begin sending reports to business unit stakeholders

Answer: (SHOW ANSWER)

NEW QUESTION: 42

When troubleshooting Enforce issues, what should be considered regarding server resources?

A. Server resources have no impact on DLP performance.

B. Server resource allocation may affect DLP system performance.

C. Server resources affect only DLP Agent functionality.

D. Server resources are managed automatically by DLP.

Answer: (SHOW ANSWER)

Enforce performance depends directly on the resources allocated to the server and its supporting database. CPU availability, memory, disk capacity, disk latency, network connectivity, and database resources can affect console responsiveness, incident persistence, reporting, policy deployment, and communication with detection servers. Resource exhaustion may appear as slow console pages, delayed incident processing, service instability, or an accumulation of incident files awaiting processing. It is incorrect to state that resources have no impact or that they affect only endpoint agents because Enforce coordinates the broader DLP environment. Symantec DLP also cannot automatically correct every operating-system, storage, or database capacity problem. Administrators must review utilization metrics and compare the deployment workload with supported sizing requirements. Therefore, option B is correct.

NEW QUESTION: 43

What detection technology supports partial contents matching?

A. Indexed Document Matching (IDM)

B. Described Content Matching (DCM)
C. Exact Data Matching (DCM)
D. Optical Character Recognition (OCR)
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 44
A divisional executive requests a report of all incidents generated by a particular region, summarized by department. What does the DLP administrator need to configure to generate this report?
A. Status attributes
B. Sender attributes
C. Custom attributes
D. User attributes
Answer: (SHOW ANSWER)

Valid 250-587 Dumps shared by EduDump.com for Helping Passing 250-587 Exam! EduDump.com now offer the **newest 250-587 exam dumps**, the EduDump.com 250-587 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 250-587 dumps with Test Engine here: https://www.edudump.com/exams/Symantec/250-587/premium/ (**110** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)